ISRCS 2008

Reliability Design Session
Axel Krings

Summary of Breakout Session

September 9-10, 2008
Idaho Falls, Idaho

Participants

- Axel Krings
- Azad Azadmanesh
- Jane Gibson
- Mike Kretzer
- Scott Bauer
- Curtis St. Michel
- Miles McQueen
- Tom Larson
- Zach Tudor
- Parag Lala
- Wayne Boyer
- Eugene Santos
- Diane Hooie
- Linda Seward

Resilient Control Systems (RCS)

❖ What is resilience?

Informal Definition of Resilience:

– Effective reconstitution of control under attack from intelligent adversaries

Resilient Control Systems

- What is the formal definition?
- The role of formal definitions
- Lessens learned from similar situations
  - E.g. the terms “Survivability” and “Survivable Systems”

- **Need workgroup on definitions**
  - **Quantifyability of resilience**

Resilient Control Systems

- Fault-tolerant Systems Design
- Design for Survivability
- Security

- What is different this time?

Beyond Survivability or Fault-tolerance

- State Awareness
- Scale of the system and dynamics
- Sophistication of recovery
- Certification requirement is significant
- Do we care about the attacks themselves?
  - The impact of ongoing attacks
  - The lack of concern for ongoing attacks

Beyond Survivability or Fault-tolerance

- ❖ Phase approach
  - – Fault tolerance (FT): from masking to recovery
  - – Resilient Control Systems (RCS): from survivability to recovery
  - – Difference is that “masking” in RCS is actually the objective of Survivability
  - – RCS approach
    - Masking => survivability
    - Recovery => transient solution towards full recovery

Analysis and Modeling

- Model Analysis
  - Balance functionality, reliability, and security
  - Interdependencies
  - Effective reconstitution of control under attack from intelligent adversaries

Analysis and Modeling

- ❖ Threats and threat Models
  - Framework of compostable threats in conjunction with the control system
  - Evolving strategies
  - “Threats” here are intelligent adversary, natural disasters, extreme event, external common mode events, etc.
  - Unintended or unanticipated usage that has collectively impact – which is outside of the functionalities tested.
  - Worse case events, pathological behaviors

Analysis and Modeling

- Failure Models
  - Hybrid fault models apply, but statistical assumptions of FT do not hold anymore
  - The probabilities have changed
  - Shift from fault-driven to event-driven
  - Is there enough room to capture all cyber threats?
    - Much discussion on this has taken place in dependability community

Analysis and Modeling

- System Analysis Models
  - Evolutionary game theory
  - Prob. Risk Assessment
  - Design for Analyzability
  - Dynamic changes over time
  - Unpredictable, Unobserved, & Unobservable Risks
  - Models that translate failure causes to the effects

  - Static models could be exploited by intelligent adversary

Appropriate Model

- The T1A1.2 Model captures the basics of control modes
  - Transient solution may be more complex
    - From “masking” towards full recovery
- The model depends on the definition
- Composable models, capturing evolving threat models and consequences

Model Parameters

- What data is available
  - Need data to parameterize models

- Potential Issues
  - Classified data
  - Parameterization of classified information
  - Usable non-classified data

Shift in Paradigms

- Shift from the *causes* to *effects* and *consequences*
- Automatic reconstitution,
  - Survivability: main focus on providing essential services, not on getting back to nominal operational levels

Path Forward

- Unification of hybrid fault models
- Relationship between fault models and system models
- Formalism, rigor
- Dealing with UUUR events
- Quantification and measurement of resilience
- Incorporating threats into models and validation
- Relationship between the reconstitution and the type of attacks

Discussion

Questions?